



**(WO/2000/010303) ACCESS CONTROL USING ATTRIBUTES CONTAINED WITHIN
PUBLIC KEY CERTIFICATES**

[Biblio. Data](#) [Description](#) [Claims](#) [National Phase](#) [Notices](#) [Documents](#)

Latest bibliographic data on file with the International Bureau

Publication Number: WO/2000/010303 **International Application No.:** PCT/IB1999/001452
Publication Date: 24.02.2000 **International Filing Date:** 30.07.1999
Chapter 2 Demand Filed: 08.03.2000

Int. Class.: H04L 12/22 (2006.01), H04L 29/06 (2006.01)

Applicant: KYBERPASS CORPORATION [CA/CA]; Suite 110 One Antares Drive Nepean, Ontario K2E 8C4 (

Inventor: HAVERTY, Rand; Kyberpass Corporation Suite 110 One Antares Drive Nepean, Ontario K2E 8C4

Agent: SEAS, Robert, J.; Sughrue, Mion, Zinn, Macpeak & Seas, PLLC Suite 800 2100 Pennsylvania Ave N.W. Washington, DC 20037-3202 (US).

Priority Data: 09/132,672 12.08.1998 US.

Title: ACCESS CONTROL USING ATTRIBUTES CONTAINED WITHIN PUBLIC KEY CERTIFICATES

Abstract: In Public Key Infrastructure ('PKI') applications, a key pair (public key and private key) is used to provide strong authentication and encryption services. The key pair is associated with the user by the use of a 'certificate,' which contains the user's public key as well as attributes associated with that user. This invention relates to the use of these attributes to control the access to a protected resource given to authenticated users. The attributes within a user's public key certificate are filtered by an attribute filter referenced by the proxy definition in order to control access to a protected resource. Further limitation of access to a protected resource is accomplished by association with server input and output addresses.

Designated AU, CA, CN, JP, SG.

States: European Patent Office (EPO) (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT SE).

Publication Language: English (EN)

Filing Language: English (EN)

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2002-523816

(P2002-523816A)

(43) 公表日 平成14年7月30日 (2002.7.30)

(51) IntCl.	識別記号	F I	テマコード (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 8 5
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 B 5 J 1 0 4
			6 7 3 A

審査請求 未請求 予備審査請求 有 (全 35 頁)

(21) 出願番号	特願2000-565651 (P2000-565651)	(71) 出願人	カイバーバス コーポレーション
(86) (22) 出願日	平成11年7月30日 (1999.7.30)		カナダ、オンタリオ ケー2イー 8シー
(85) 翻訳文提出日	平成13年2月9日 (2001.2.9)		4、ネビアン、ワン アンタレス ドライ
(86) 国際出願番号	PCT/IB99/01452		ブ (番地なし)、スイート110
(87) 国際公開番号	WO00/10303	(72) 発明者	ヘーバティ、ランド
(87) 国際公開日	平成12年2月24日 (2000.2.24)		カナダ、オンタリオ ケー2イー 8シー
(31) 優先権主張番号	09/132, 672		4、ネビアン、ワン アンタレス ドライ
(32) 優先日	平成10年8月12日 (1998.8.12)		ブ (番地なし)、スイート110、カイバ
(33) 優先権主張国	米国 (US)		ーバス コーポレーション
(81) 指定国	EP (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, I T, LU, MC, NL, PT, SE), AU, CA, C N, J P, S G	(74) 代理人	弁理士 北澤 一浩 (外2名)
		Fターム (参考)	5B085 AE03 AE09
			5J104 AA07 KA05 NA02 NA05 PA07

(54) 【発明の名称】 公開鍵証明書に含まれたアトリビュートを使用するアクセス制御

(57) 【要約】

公開鍵インフラストラクチャ (PKI) の応用で、一対の鍵 (公開鍵と非公開鍵) を使用して強力な認証と暗号化サービスを提供する。一対の鍵は、ユーザの公開鍵とユーザに関連させたアトリビュートを含む「証明書」の使用によりユーザと関連させる。本発明はそのアトリビュートを使用して、認証したユーザに保護リソースへのアクセスを制御する。ユーザ公開鍵証明書内のアトリビュートは保護リソースへのアクセスを制御するためにプロキシ定義により参照したアトリビュート・フィルタによってフィルタ処理される。保護リソースへのアクセスの別な制限はサーバ入力と出力アドレスに関連させておこなう。

【特許請求の範囲】

【請求項1】 クライアント・ステーションのユーザからコンピュータ・リソースへのアクセス要求のサーバ認証方法において、

上記サーバに上記ユーザに関連するアトリビュートを含む証明書を記憶させるステップと、

上記サーバにアトリビュート・フィルタを記憶させるステップと、

上記アトリビュート・フィルタを使用して上記証明書のアトリビュートから算出値を上記サーバで演算するステップと、

上記算出値が上記クライアント・ステーションのユーザを認証するかどうか上記サーバで判定するステップと、

上記コンピュータ・リソースへのアクセスを上記算出値が許可するか、あるいは拒絶するか上記サーバで判定するステップとを有することを特徴とするアクセス要求のサーバ認証方法。

【請求項2】 上記サーバにアトリビュート・フィルタを記憶させる上記ステップは、

上記アトリビュート・フィルタの識別を判定するステップと、

上記コンピュータ・リソースへのアクセス制御用に使用するために上記証明書から上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュートを評価するために数学的シーケンスを判定するステップとを有することを特徴とする、請求項1に記載のアクセス要求のサーバ認証方法。

【請求項3】 上記演算するステップは、

上記証明書を検索するために上記サーバを探索するステップと、

上記証明書が上記サーバに見つからないなら遠隔の証明書保存部を探索するステップと、

上記証明書が在った時に上記証明書を検索するステップとを有することを特徴とする、請求項1に記載のアクセス要求のサーバ認証方法。

【請求項4】 上記演算するステップは、

上記証明書の中の使用可能なアトリビュートの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記アトリビ

ュートを選択するステップと、

上記アトリビュート・フィルタを評価することにより上記算出値を判定するステップとを有することを特徴とする、請求項1に記載のアクセス要求のサーバ認証方法。

【請求項5】 クライアント・ステーションのユーザからコンピュータ・リソースへのアクセス要求のサーバ認証の方法において、

上記サーバに上記ユーザに関連するアトリビュートを含む証明書を記憶させるステップと、

上記サーバにアトリビュート・フィルタを記憶させるステップと、

上記サーバにプロキシ定義を記憶させるステップと、

上記アトリビュート・フィルタを使用して上記証明書のアトリビュートから導いた算出値を上記サーバで演算するステップと、

上記算出値が上記クライアント・ステーションのユーザを認証するかどうか上記サーバで判定するステップと、

上記コンピュータ・リソースへのアクセスを上記算出値が許可するか、あるいは拒絶するか上記サーバで判定するステップとを有することを特徴とするアクセス要求のサーバ認証方法。

【請求項6】 上記サーバにアトリビュート・フィルタを記憶させる上記ステップは、

上記証明書内の使用可能なアトリビュートを判定するステップと、

上記コンピュータ・リソースへのアクセス制御用に使用するために上記証明書から上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュートを評価するために数学的シーケンスを判定するステップとを有することを特徴とする、請求項5に記載のアクセス要求のサーバ認証方法。

【請求項7】 上記サーバにプロキシ定義を記憶させるステップは、上記アトリビュート・フィルタを参照するプロキシ定義要素を付加するステップを含むことを特徴とする、請求項5に記載のアクセス要求のサーバ認証方法。

【請求項8】 上記ユーザに関連したアトリビュートを含む証明書を上記サーバに記憶させるステップは、

上記証明書を検索するために上記サーバを探索するステップと、

上記証明書が上記サーバに見つからないなら遠隔の証明書保存部を探索するステップと、

上記証明書が在った時に上記証明書を検索するステップとを有することを特徴とする、請求項5に記載のアクセス要求のサーバ認証方法。

【請求項9】 上記演算するステップは、

上記プロキシ定義により参照した上記アトリビュート・フィルタの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュート・フィルタを評価することにより上記算出値を判定するステップとを有することを特徴とする、請求項5に記載のアクセス要求のサーバ認証方法。

【請求項10】 上記演算するステップは、

上記プロキシ定義により参照した上記アトリビュート・フィルタの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュート・フィルタと上記サーバの入力アドレスを使用して上記選択したアトリビュートを評価することにより、上記算出値を判定するステップとを有することを特徴とする、請求項5に記載のアクセス要求のサーバ認証方法。

【請求項11】 上記演算するステップは、

上記プロキシ定義により参照した上記アトリビュート・フィルタの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュート・フィルタと上記保護コンピュータ・リソースの出力アドレスを使用して上記選択したアトリビュートを評価することにより上記算出値を判定するステップとを有することを特徴とする、請求項5に記載のアクセス要求

のサーバ認証方法。

【請求項12】 クライアント・ステーションのユーザから、コンピュータ・リソースへのアクセス要求の認証に適したコンピュータ・システムにおいて、プロセッサとメモリから成り、

上記コンピュータ・システムに上記ユーザに関連するアトリビュートを含む証明書記憶させるステップと、

上記コンピュータ・システムにアトリビュート・フィルタを記憶させるステップと、

上記アトリビュート・フィルタを使用して上記証明書のアトリビュートから算出値を上記コンピュータ・システムで演算するステップと、

上記算出値が上記クライアント・ステーションのユーザを認証するかどうか上記コンピュータ・システムで判定するステップと、

上記コンピュータ・リソースへのアクセスを上記算出値が許可するか、あるいは拒絶するか上記コンピュータ・システムで判定するステップとを、

上記コンピュータ・システムが実行可能となるようにしたソフトウェア・インストラクションを上記メモリが含むことを特徴とするアクセス要求の認証に適したコンピュータ・システム。

【請求項13】 上記メモリは、上記コンピュータ・システムが更に、上記アトリビュート・フィルタの識別を判定するステップと、上記コンピュータ・リソースへのアクセス制御用に使用するために上記証明書から上記ユーザアトリビュートを選択するステップと、上記アトリビュートを評価するために数学的シーケンスを判定するステップとを、

実行可能となるソフトウェア・インストラクションを有することを特徴とする、請求項12に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項14】 上記メモリは、上記コンピュータ・システムが更に、上記証明書を検索するために上記コンピュータ・システムを探索するステップと、

上記証明書が上記コンピュータ・システムに見つからないなら遠隔の証明書保

存部を探索するステップと、

上記証明書が在った時に上記証明書を検索するステップとを、

実行可能となるソフトウェア・インストラクションを有することを特徴とする
、請求項12に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項15】 上記メモリは、上記コンピュータ・システムが更に、

上記証明書の中の使用可能なアトリビュートの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記アトリビ
ュートを選択するステップと、

上記アトリビュート・フィルタを評価することにより上記算出値を判定するス
テップとを、

実行可能となるソフトウェア・インストラクションを更に有することを特徴と
する、請求項12に記載のアクセス要求の認証に適したコンピュータ・システム
。

【請求項16】 クライアント・ステーションのユーザから、コンピュータ
・リソースへのアクセス要求の認証に適したコンピュータ・システムにおいて、
プロセッサとメモリから成り、

上記コンピュータ・システムに上記ユーザに関連するアトリビュートを含む証
明書を記憶させるステップと、

上記コンピュータ・システムにアトリビュート・フィルタを記憶させるステッ
プと、

上記コンピュータ・システムにプロキシ定義を記憶させるステップと、

上記アトリビュート・フィルタを使用して上記証明書のアトリビュートから算
出値を上記コンピュータ・システムで演算するステップと、

上記算出値が上記クライアント・ステーションのユーザを認証するかどうか上
記コンピュータ・システムで判定するステップと、

上記コンピュータ・リソースへのアクセスを上記算出値が許可するか、あるい
は拒絶するか上記コンピュータ・システムで判定するステップとを、

上記コンピュータ・システムが実行可能となるようにしたソフトウェア・イン
ストラクションを上記メモリが含むことを特徴とするアクセス要求の認証に適し

たコンピュータ・システム。

【請求項17】 上記証明書内で使用可能なアトリビュートを判定するステップと、

上記コンピュータ・リソースへのアクセス制御用に使用するために上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュートを評価するために数学的シーケンスを判定するステップとを有するように、上記コンピュータ・システムでアトリビュート・フィルタを記憶させるステップを更に該コンピュータ・システムが実行可能となるようにしたソフトウェア・インストラクションを上記メモリが更に有することを特徴とする、請求項16に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項18】 上記アトリビュート・フィルタを参照するブロック定義要素を付加するステップを有するように、ブロック定義を記憶させるステップを上記コンピュータ・システムが更に実行可能となるようにしたソフトウェア・インストラクションを上記メモリが更に有することを特徴とする、請求項16に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項19】 上記証明書を検索するために上記コンピュータ・システムを探索するステップと、

上記証明書が上記コンピュータ・システムに見つからないなら遠隔の証明書保存部を探索するステップと、

上記証明書が在った時に上記証明書を検索するステップとを有するように、上記コンピュータ・システムで上記ユーザと関連したアトリビュートを含む証明書を記憶させるステップを更に該コンピュータ・システムが実行可能となるようにしたソフトウェア・インストラクションを上記メモリが更に有することを特徴とする、請求項16に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項20】 上記証明書の中の使用可能なアトリビュートの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記アトリビュートを選択するステップと、

上記アトリビュート・フィルタを評価することにより上記算出値を判定するステップとを有するように、上記コンピュータ・システムが演算ステップを更に実行可能となるようにしたソフトウェア・インストラクションを上記メモリが更に有することを特徴とする、請求項16に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項21】 上記ブロック定義により参照した上記アトリビュート・フィルタの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュート・フィルタと上記コンピュータ・システムの入力アドレスを使用して上記選択したアトリビュートを評価することにより上記算出値を判定するステップとを有するように、上記コンピュータ・システムが演算ステップを更に実行可能となるようにしたソフトウェア・インストラクションを上記メモリが更に有することを特徴とする、請求項16に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項22】 上記ブロック定義により参照した上記アトリビュート・フィルタの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュート・フィルタと上記保護コンピュータ・リソースの出力アドレスを使用して上記選択したアトリビュートを評価することにより上記算出値を判定するステップとを有するように、上記コンピュータ・システムが演算ステップを更に実行可能となるようにしたソフトウェア・インストラクションを上記メモリが更に有することを特徴とする、請求項16に記載のアクセス要求の認証に適したコンピュータ・システム。

【請求項23】 クライアント・ステーションのユーザから、コンピュータ・リソースへのアクセス要求の認証をコンピュータができるためのコンピュータ・プログラム製品において、

上記コンピュータが所定のオペレーションをおこなうことが可能なソフトウェ

ア・インストラクションと、該インストラクションを運ぶコンピュータ読み取り可能な媒体とを有し、

上記所定オペレーションは、

上記コンピュータに上記ユーザに関連するアトリビュートを含む証明書を記憶させるステップと、

上記コンピュータにアトリビュート・フィルタを記憶させるステップと、

上記アトリビュート・フィルタを使用して上記証明書のアトリビュートから算出値を上記コンピュータで演算するステップと、

上記算出値が上記クライアント・ステーションのユーザを認証するかどうか上記コンピュータで判定するステップと、

上記コンピュータ・リソースへのアクセスを上記算出値が許可するか、あるいは拒絶するか上記コンピュータで判定するステップとを含むことを特徴とするアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項24】 上記コンピュータにアトリビュート・フィルタを記憶させる上記ステップは、

上記アトリビュート・フィルタの識別を判定するステップと、

上記コンピュータ・リソースへのアクセス制御用に使用するために上記証明書から上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュートを評価するために数学的シーケンスを判定するステップとを有することを特徴とする、請求項23に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項25】 上記ユーザと関連したアトリビュートを含む証明書を上記サーバに記憶するステップは、

上記証明書を検索するために上記サーバを探索するステップと、

上記証明書が上記サーバに見つからないなら遠隔の証明書保存部を探索するステップと、

上記証明書が在った時に上記証明書を検索するステップとを有することを特徴とする、請求項23に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項26】 上記アトリビュート・フィルタを使用して上記証明書内の
上記アトリビュートから算出値を上記サーバで演算するステップは、

上記証明書の中の使用可能なアトリビュートの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記アトリビ
ュートを選択するステップと、

上記アトリビュート・フィルタを評価することにより上記算出値を判定するス
テップとを有することを特徴とする、請求項23に記載のアクセス要求の認証を
おこなうことのできるコンピュータ・プログラム製品。

【請求項27】 クライアント・ステーションのユーザから、コンピュータ
・リソースへのアクセス要求の認証をコンピュータができるためのコンピュータ
・プログラム製品において、

上記コンピュータが所定のオペレーションをおこなうことが可能なソフトウェ
ア・インストラクションと、該インストラクションを運ぶコンピュータ読み取り
可能な媒体とを有し、

上記所定オペレーションは、

上記コンピュータに上記ユーザに関連するアトリビュートを含む証明書を記憶
させるステップと、

上記コンピュータにアトリビュート・フィルタを記憶させるステップと、

上記コンピュータにプロキシ定義を記憶させるステップと、

上記アトリビュート・フィルタを使用して上記証明書のアトリビュートから算
出値を上記コンピュータで演算するステップと、

上記算出値が上記クライアント・ステーションのユーザを認証するかどうか上
記コンピュータで判定するステップと、

上記コンピュータ・リソースへのアクセスを上記算出値が許可するか、あるい
は拒絶するか上記コンピュータで判定するステップとを有することを特徴とする
、アクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項28】 上記コンピュータにアトリビュート・フィルタを記憶させ
る上記ステップは、

上記証明書内で使用可能なアトリビュートを判定するステップと、

上記コンピュータ・リソースへのアクセス制御用に使用するために上記証明書から上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュートを評価するために数学的シーケンスを判定するステップとを有することを特徴とする、請求項27に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項29】 上記コンピュータにプロキシ定義を記憶させるステップは、上記アトリビュート・フィルタを参照するプロキシ定義要素を付加するステップを含むことを特徴とする、請求項27に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項30】 上記ユーザに関連したアトリビュートを含む証明書を上記コンピュータに記憶させるステップは、

上記証明書を検索するために上記コンピュータを探索するステップと、

上記証明書が上記コンピュータに見つからないなら遠隔の証明書保存部を探索するステップと、

上記証明書が在った時に上記証明書を検索するステップとを有することを特徴とする、請求項27に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項31】 上記アトリビュート・フィルタを使用して上記証明書内の上記アトリビュートから得た算出値を上記サーバで演算するステップは、

上記プロキシ定義により参照した上記アトリビュート・フィルタの検索ステップと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記ユーザ・アトリビュートを選択するステップと、

上記アトリビュート・フィルタを評価することにより上記算出値を判定するステップとを有することを特徴とする、請求項27に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項32】 上記アトリビュート・フィルタを使用して上記証明書内の上記アトリビュートから得た算出値を上記サーバで演算するステップは、

上記プロキシ定義により参照した上記アトリビュート・フィルタの検索ステッ

ブと、

上記アトリビュート・フィルタにより求められた上記証明書内の上記アトリビュートを選択するステップと、

上記アトリビュート・フィルタと上記サーバの入力アドレスを使用して上記選択したアトリビュートを評価することにより上記算出値を判定するステップを有することを特徴とする、請求項27に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【請求項33】 上記アトリビュート・フィルタを使用して上記証明書内の上記アトリビュートから得た算出値を上記サーバで演算するステップは、

上記アトリビュート・フィルタにより求められた上記証明書内の上記アトリビュートを選択するステップと、

上記アトリビュート・フィルタと上記保護リソースの出力アドレスを使用して上記選択したアトリビュートを評価することにより上記算出値を判定するステップとを有することを特徴とする、請求項27に記載のアクセス要求の認証をおこなうことのできるコンピュータ・プログラム製品。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、公開鍵証明書とプロキシ定義内に含まれたユーザ・アトリビュートに基づいた、保護されたリソースへのアクセスを制御する方法に関する。また、本発明は公開鍵証明書とプロキシ定義内に含まれたユーザ・アトリビュートに基づいた、保護リソースへのアクセスを制御するソフトウェアを有するプログラム製品に関する。さらに、本発明は公開鍵証明書とプロキシ定義内に含まれたユーザ・アトリビュートに基づいた、保護リソースへのアクセスを制御するためのオペレーションをおこなうコンピュータ・システムに関する。

【0002】

【従来の技術】

公開鍵インフラストラクチャ（パブリック・キー・インフラストラクチャ：PKI）技術の出現前には、保護コンピュータ・リソースへの複数のユーザのアクセスを制御するために、トランザクション・プログラムの実行やデータベースをホスト化するなどの、いくつかの技術が発展した。保護方法の一つは物理的手段により保護対象のコンピュータ・システムへの認可されていないアクセスを防ぐことであった。この種の方法のうち最も簡単なものは、保護コンピュータ・システムにつながる端末へのアクセスを制限することであった。別の方法は、保護コンピュータ・システムと公共コンピュータ・ネットワーク間の物理的なネットワーク接続を許可しないことにより、認可していないアクセスを防ぐことであった。さらに別の保護方法は、保護コンピュータ・システムあるいは保護サーバの各々について自動的なアクセス制御システムを履行することであった。効果はあるが、これらの技術はコンピュータ・リソースの効果的な利用を抑制するという重大な欠点を抱えている。物理的なセキュリティ方法の場合には、インターネットのような公共ネットワークを保護コンピュータ・システムへのアクセスのために利用する機会が失われる。同様に、サーバ・レベルで履行される自動アクセス制御システムは特定のサーバにだけ適用可能である。つまり、アクセス制御の権利の管理はいくつかのサーバ間で重複することになり、間違いや混乱を発生し、また最

最終的にコストの増大につながる。

【0003】

インターネットおよび各種法人のイントラネットのような公共ネットワークの長所を生かすために、産業界はセキュリティ施策を実行するためのセキュリティ・サーバを利用する方法を採用している。セキュリティ・サーバは保護コンピュータ・リソースとクライアント・ステーション間に配置され、リソースとクライアント間の単独リンクとして働く。クライアントはセキュリティ・サーバに直接接続させることが可能であり、あるいは1個以上の通信ルータを介してセキュリティ・サーバにリンクさせることが考えられる。さらに、セキュリティ・サーバは単独のリソースまたは複数のリソースを保護することも可能である。ユーザが適切に認証される時のみ、このセキュリティ・サーバは保護リソースとクライアント・ステーション間の通信リンクを確立することになる。「セキュリティ・サーバ」という用語は、この意味において、セキュリティ・サーバ、ファイアウォール、プロキシ（代理）サーバ、認証サーバ等を含む。さらに、「保護リソース」という用語は保護対象のデータベース・サーバ、アプリケーション・サーバおよびトランザクション・サーバを含むが、これらに限定されない。

【0004】

セキュリティ・サーバと組み合わせる方策は公開鍵インフラストラクチャ（PKI）技術である。PKIの適用では、公開鍵と非公開鍵の一对の鍵（パブリック・キーとプライベート・キー）を使用して強力な認証と暗号化作業をおこなう。この一对の鍵はユーザについてのアトリビュートに加え、ユーザの公開鍵を含む「証明書」の使用によりユーザと関連づけられる。セキュリティ・サーバはプロキシを確立することによりクライアント・ステーション（あるいは通信ルータ）と保護リソース間のリンクを設立する。このプロキシは、クライアント・ステーションが適切に認証される場合にだけ作動させる。通常、このクライアント・ステーション認証は、クライアント・ステーションが公開鍵にアクセスするために正確なパスワードの提示、および実際の非公開鍵の入手に基礎をおいている。

【0005】

【発明が解決しようとする課題】

本発明の目的は公開鍵証明書に記憶させたアトリビュートに基づいたセキュリティ・サーバにおいてアクセス制御機能を加える方法を提供する。公開鍵証明書に記憶させたどのアトリビュートもセキュリティ・サーバを介して保護リソースへのアクセスを制御するために使用できる。

【0006】

【課題を解決するための手段】

本発明によれば、セキュリティ・サーバを介するアクセスを許可あるいは拒絶する新規な方法は、アトリビュートの値に基盤を置く。すなわち本発明の方法は、アトリビュートの値に基づいた条件をセキュリティ・サーバ内のプロキシと直接関連させるようにする。クライアント・ステーションと保護リソース間のプロキシはアクセス要求者が認証された時、および、そのプロキシに関連したアトリビュート条件が満たされる時のみ確立される。

【0007】

本発明によれば、セキュリティ・サーバを介して保護リソースへのアクセスを制限する新規な方法はプロキシ定義と関連させた入出力アドレスに基づいたものである。すなわち本発明の方法は、アドレスに基づいた条件が特定のリソースにたいしてだけのアクセスを制限できるようにしたものである。

【0008】

【発明の実施の形態】

本発明の望ましい実施の形態を、初めにイントラネットのような内部ネットワークから保護リソースにアクセスするクライアント・ステーションについて説明する。その後、インターネット、あるいは他の同様な公共ネットワークのような外部ネットワークから保護リソースにアクセスするクライアント・ステーションについて説明する。これら2種の望ましい実施の形態は、この2種の応用だけでなく、他の広範囲な環境に対しても適用可能である。つまり、この実施の形態は極めて一般的な意味で本発明を例示する役割を果たすことになる。

【0009】

セキュリティ・サーバ方法

セキュリティ・サーバ方法は図1に簡潔に示してある。図中100のクライア

ント・ステーションは、汎用あるいは特製コンピュータ・システムにて実行するプロセスと理解することができる。プロセスとしてのクライアント・ステーション100は、保護リソース上のアプリケーションに関するタスクの実行を要求するユーザと考えることができる。

【0010】

図1では、101がセキュリティ・サーバを示し、102は保護リソースを示す。図1から分かるように、クライアント・ステーション100と保護リソース102間には直接の通信リンクは存在しない。セキュリティ・サーバ101は汎用あるいは特製コンピュータ・システムで走行するプロセスと考えられる。同様に、保護リソース102もプロセスと考えられる。

【0011】

保護リソース102へのアクセスを望むユーザは、セキュリティ・サーバ101を介してユーザのクライアント・ステーション100からアクセスしなくてはならない。保護リソース102へのアクセスが認可されたユーザはセキュリティ・サーバ101により認証を受け、保護リソース102を利用することを許可される。セキュリティ・サーバ101は認可を受けてないユーザの保護リソース102へのアクセスを防止する。

【0012】

図2はより洗練されたコンピュータ・ネットワークを示し、おそらく現行の環境において一般的に見られるものである。クライアント・ステーション100は保護リソース102へ到達可能な2つの経路を有する。

【0013】

最短の経路はセキュリティ・サーバ101への通信ルータ112を経由する接続である。セキュリティ・サーバ101によりユーザが適切に認証を受けると、プロキシを経由して保護リソース102へのアクセスが許可される。通信ルータ112の唯一の役割はクライアント・ステーション100とセキュリティ・サーバ101間の接続を容易にすることである。

【0014】

別の経路は通信ルータ111を経由してファイアウォール113への接続を確

立するものである。ファイアウォール113は通信リンクをサポートし、セキュリティ・サーバ101と同じようにしてイントラネット114へのアクセスを提供する。これは関連のリソースが外部的にアクセスできるのに加え内部的にもアクセス可能となることを考えると、近代的な方法である。イントラネット114はセキュリティ・サーバ101に物理的に接続されている。ユーザがイントラネット114にアクセスすることが許可されたなら、セキュリティ・サーバ101は保護リソースへの認可されていない割り込みを妨げる。ユーザが本物であり適切に認証されるなら、プロキシを経由して保護リソース102へのアクセスが許可される。見て分かるように、図2は今日のコンピュータ環境で考えられる潜在的なネットワークの組み合わせ全てを示しているわけではない。理解を容易にするため、「クライアント・ステーション」という用語は、ユーザが現在アクセスしているコンピュータ・システムだけではなく、クライアント・ステーション100とセキュリティ・サーバ101間にあるシステム全て（例えば、通信ルータ、ファイアウォール、イントラネット）を含むものとする。

【0015】

クライアント・ステーション100、セキュリティ・サーバ102、保護リソース103など全てが走行するコンピュータ・システムは、一般的には、かなりの距離を取って離れた物理的に異なったコンピュータ・システムである。この配列は一つの典型例ではあるが、上記3つのプロセスが物理的に異なったコンピュータ・システム上を走行しない時、あるいは、かなり距離を取って離れたコンピュータ・システムでない時でさえもこのセキュリティ・サーバ方式のコンセプトを適用する。しかし、この説明の一般的に意味するものは、ここに説明した典型的配列に関することである。

【0016】

このコンピュータ・システムが通信する方法は高い水準で取り扱われ、その詳細は本発明を分かり易くするため省略する。この通信についての詳細な情報は、「データおよびコンピュータ・通信 (Data and Computer Communications)」あるいは「ローカル・ネットワーク (Local Networks)」を参照することで得られる。両文献は共にウィリアム

・ストーリーングスによる著作であり、その全体は本出願の有用な背景情報の引用文献として示す。

【0017】

実用レベルでのプロセス（クライアント・プロセス、セキュリティ・サーバ・プロセスおよびアプリケーション・サーバ・プロセスなどを含む）は様々な媒体の一つでソフトウェアとして供給される。さらに、実際のソフトウェアはプログラム言語あるいはプログラム言語で書かれた文書に基づくものである。こうしたプログラム言語文書はコンピュータにより実行した時に、その文書の特定の内容に基づいてコンピュータを作動させ、所定の方法で限定的なプロセスを走行させる。また、ソフトウェアは、オリジナルのソース・コード、アセンブリ・コード、オブジェクト・コード、機械言語、それらの圧縮化バージョンあるいは暗号化バージョン、などを含む。但し、これらに限定されない多数の形で提供することが考えられる。

【0018】

コンピュータ・システムにおいて良く知られているものは「媒体」あるいは本願で使用する「コンピュータ読み取り可能媒体」であり、具体的にはフロッピー（登録商標）ディスク、磁気テープ、コンパクト・ディスク、集積回路、カートリッジ、通信回路を介する遠隔伝送、またはコンピュータで使用可能な他の同様な媒体である。例えば、プロセスを定義するソフトウェアを供給するためには、供給者はフロッピーディスクを提供するか、衛星通信や直接の電話回線やインターネットなどを介して、様々な形のソフトウェアを伝送することが考えられる。

【0019】

こうしたソフトウェア・インストラクションはフロッピーディスクに「書き込まれる」か、集積回路に「記憶させる」か、通信回路で「運搬される」かであるが、ここでの説明の目的から考慮すると、コンピュータで使用可能な媒体はソフトウェアを「運ぶ」と称することにする。このように、「運ぶ」という用語はソフトウェアがコンピュータで使用可能な媒体に関連させる上記方法および同等の全ての方法を含むものである。

【0020】

従って、説明を分かり易くするため、「プログラム製品」という用語は、これ以後、上記のようにソフトウェアを適切な方法で運ぶコンピュータで使用可能な媒体に関して使用する。

【0021】

プロキシ

図1では、セキュリティ・サーバ101の入力アドレスはクライアント・ステーション100とのインターフェースを有する。セキュリティ・サーバ101の出力アドレスは保護リソース102とのインターフェースを有する。セキュリティ・サーバ101にあるプロキシ定義は、セキュリティ・サーバ101の出力アドレスとセキュリティ・サーバ101の入力アドレス間の正確な対応を条件として指定する。プロキシ定義に含まれた情報は、どのように入力アドレスのトラフィックが指定された出力アドレスに経路を定められるかを決定する。さらに、プロキシ定義に含まれたこの情報が、プロキシ定義に含まれる全ての要素が考慮されることを確実にする。

【0022】

プロキシ定義は、以下に示すようなプライバシー、セキュリティ、およびアクセス制御に関する多くの要素を有する。

1. 記号プロキシ名。
2. FTPやHTTPのような関連したプロトコル。
3. 接続に含むべき、あるいは除外すべきアドレスを特定する入力アドレス（例えば、TCP/IP）フィルタ。
4. クライアントとサーバ間の全てのユーザおよび/あるいはデータのトラフィックを示す認証。
5. クライアントとサーバ間の全トラフィックを出所で暗号化し、送り先で解読することを示す暗号化。
6. クライアントとサーバ間の全トラフィックを出所で圧縮し、送り先で復帰（圧縮解除）することを示す圧縮。
7. 入力アドレス（セキュリティ・サーバのクライアント・ステーション側のアドレス）。

8. 出力アドレス（保護リソースに接続したセキュリティ・サーバの「保護」側のアドレス）

9. 保護リソース・アドレス（どのプロキシに対してもいくつかある）。

【0023】

証明書

表1はX. 509バージョン3の公開鍵証明書の構成を示している。

【0024】

【表1】

表 1 (X. 509 証明書)

証明書バージョン番号
証明書シリアル番号
証明書発行者の識別名アトリビュート
有効日付／時間以前不可／以後不可
被証明者の識別名アトリビュート
被証明者の公開鍵ビット
追加アトリビュート
発行者のデジタル署名ビット

【0025】

アトリビュートのタイプ、証明書発行者と被証明者（証明書所有者）識別名を含む数値申し立て、有効日付、追加アトリビュートなどは、経路パスを制御したり、あるいは分離セキュリティ施策ドメイン用の規則を定義するためにセキュリティ・サーバによって使用可能である。例えば、ある仮想の会社がそれぞれ保護サーバを有する3つの、管理、製造、エンジニアリング部門があるとする。その保護サーバへのアクセスはセキュリティ・サーバを介する。管理部門のスタッフは自己の業務を達成するために管理サーバと製造サーバへのみアクセス可能である。エンジニアリング部門のスタッフは製造サーバとエンジニアリング・サーバへのアクセスが可能である。製造部門のスタッフは製造サーバへのアクセスのみ可能である。

【0026】

標準的なX. 509「組織ユニット名」アトリビュートは、従業員が当会社内のどこで働くかを示すために使用可能である。例えば、エンジニアリング部門で働くジョン・ドウは、一般名=ジョン・ドウ、組織ユニット名=エンジニアリング、組織名=ハイポ・コーポレーション（仮想会社）等の識別名を有する。経理課で働いているジェーン・ドウは、一般名=ジェーン・ドウ、組織ユニット名=管理、組織名=ハイポ・コーポレーション（仮想会社）等の識別名を有する。

【0027】

この仮想会社では、セキュリティ・サーバは別々に各保護サーバに接続させてある。セキュリティ・サーバは、その発生点に拘わらず、従業員からの全ての接続要求を認証する。この従業員の組織ユニット名アトリビュート値がユーザのアクセス許可を判定するためにセキュリティ・サーバによって使われる。例えば、「エンジニアリング」の組織ユニット・アトリビュート値を持っている従業員だけがエンジニアリング・サーバへの接続を許可される。

【0028】

証明書とアトリビュートの説明は「安全な電子商取引（Secure Electronic Commerce）」、W. フォード（Ford）とM. S. ボーム（Baum）著、に見られる。証明書に含まれたアトリビュートは、一般名、地方名、州名あるいは郡名、組織名、組織ユニット名、国名、および街路住所などである（これに限定されない）。

【0029】

認証手続き

図4はPKIシステムに使用した、高レベル・ステップに変えた認証手続きを示す。これは一般化した手続きであり、認証手続きにおけるアトリビュート・フィルタを使用することをユーザに示すため用いる。

【0030】

初めのステップ200では、クライアント・ステーション100がセキュリティ・サーバ101の公然のものとなったプロキシ・アドレスへの接続を求める。通信ルータ111と112、ファイアウォール113、イントラネット114は分かり易くするため図4から除外してある。前述のように、セキュリティ・サー

バ101へのアクセス要求はさまざまな経路をたどることができる。

【0031】

ステップ201では、セキュリティ・サーバ101はクライアント・ステーション100からの接続要求を受け入れる。接続要求の受け入れ後、ステップ202ではセキュリティ・サーバはクライアント・ステーション100にログイン識別とパスワードを求める。

【0032】

ステップ203では、セキュリティ・サーバ101からのログイン識別要求の受領により、クライアント・ステーション100はユーザが非公開鍵の適切な保有者かどうか判定を求められる。クライアント・ステーション100はユーザが非公開鍵を所有しており、しかも、ユーザがその鍵を適切に使用する必要な知識を有することを検証しなくてはならない。ユーザが適切に非公開鍵を使用できるなら、クライアント・ステーション100はセキュリティ・サーバ101にユーザが非公開鍵を持っており、その鍵を適切に使用する知識があることを伝える。

【0033】

ステップ204では、セキュリティ・サーバ101がユーザの公開鍵証明書に対してユーザのログオン情報を認証する。公開鍵証明書はセキュリティ・サーバ101あるいは遠隔の証明書保存場所に記憶させてある。公開鍵証明書が遠隔の保存場所に記憶させてあるなら、セキュリティ・サーバ101は認証手続きに入る前に公開鍵証明書を検索する。

【0034】

ステップ205では、セキュリティ・サーバ101はユーザを検証すべきかどうか判定をおこなう。ステップ206では、ユーザが検証されたなら、保護リソースへのアクセスが許可される。それ以外は、ステップ207で、認証エラーのためにユーザが検証されないでクライアント・ステーション100からの接続が無効となる。

【0035】

アトリビュート・フィルタ

本発明では、アトリビュート・フィルタとして知られている別の要素をブロック

シ定義に加える。このアトリビュート・フィルタの目的はユーザの公開鍵証明書にある特定のアトリビュート値に基づきセキュリティ・サーバ100を介してアクセスを制御することである。セキュリティ・サーバ100により使用されるプロキシ定義は、その一つがアトリビュート・フィルタ定義である一組の上記要素群から成る。アトリビュート・フィルタ定義はフィルタ名と「アクセス演算式」から成る。アトリビュート・フィルタ名はプロキシ定義にハード・コード化することが可能であるが、柔軟性は犠牲になる。アクセス演算式はブール演算式である（この演算式を書くための表記法の一つはインターネットRFC1960で定義したような「逆ポーランド表記法」であり、他の表記法も可能である。）

【0036】

セキュリティ・サーバ101を介する保護リソース102へのアクセスは、アクセス演算式のブール演算式が接続要求時に本物と評価する時に認可される。アトリビュート・フィルタ用の簡単なブール演算式の一例は「CN=Kelly（ケリー）」である。この例では、接続を確立することを試みる要求者の一般名（CN）が「ケリー」であるなら、保護リソース102へのアクセスは許可されることになる。アトリビュート・フィルタ演算のアクセス演算式の演算は本物評価に限定されない、すなわち、保護リソース102へのアクセスはアクセス演算式が本物と評価したなら拒絶される可能性がある。

【0037】

図5は、セキュリティ・サーバ101が公開鍵証明書に含まれるアトリビュートを評価する演算を実行する高水準ステップを示している。ステップ301では、セキュリティ・サーバ101がログオン要求（図4のステップ204を参照）を認証するため始動すると、記憶部から公開鍵証明書を検索する。ステップ302では、セキュリティ・サーバ101は公開鍵証明書が局地的に保存されているか、遠隔地に保存されているか判定する。遠隔地ならば、ステップ303は遠隔地記憶部から証明書を検索する。

【0038】

ステップ304では、公開鍵証明書が検索されると、セキュリティ・サーバ101はクライアント・ステーション100が要求したプロキシ定義を評価する。

セキュリティ・サーバ101は要求にあった特定の入力/出力アドレス指定に使用するプロキシ定義によって、どのアトリビュート・フィルタが求められているか判定しなくてはならない。前述のように、プロキシ定義は特定のプロキシ定義に適したアトリビュート・フィルタに対するポインタを含む。

【0039】

ステップ305では、プロキシ定義により特定されたアトリビュート・フィルタを判定した後、セキュリティ・サーバ101はアトリビュート・フィルタ内のアクセス演算式を使用してアトリビュート・フィルタ内に並べられた特定の公開鍵証明書を評価する。アクセス演算式は様々な表記法で書かれる。インターネットRFC1960表記法だけの使用に限定されない。

【0040】

ステップ306では、アクセス演算式が本物と評価したなら、次にステップ308では、セキュリティ・サーバ101は保護リソース102へのアクセスを許可する。それ以外、アクセス演算式が偽物と評価したら、ステップ307でセキュリティ・サーバ101は保護リソース102へのアクセスを拒絶する。前記のように、アクセスはアトリビュート・フィルタの初期セットアップに基づき、ステップ306が本物と評価する時にも拒絶される可能性がある。

【0041】

入力/出力アドレス

アトリビュート・フィルタを使用する別の実施の形態は、プロキシ定義の入力アドレス要素あるいは出力アドレス要素と関連させてある。この組み合わせは保護リソースへのアクセスに対し、さらに制限するために使用できる。アトリビュート・フィルタが入力アドレス（セキュリティ・サーバ101のクライアント側）と組み合わせられ、しかもアクセス演算式が本物と評価したなら、セキュリティ・サーバを介する保護リソース102へのアクセスは出力アドレス（セキュリティ・サーバ101の保護側）で許可される、あるいは拒絶されることになる。アトリビュート・フィルタと出力アドレスを組み合わせることは保護リソース102へのアクセスを抑制する。アクセス演算式が本物と評価したなら、プロキシの出力側で特定の保護サーバ・アドレスでの保護リソース102へのセキュリティ

ィ・サーバ101を介するアクセスは許可される、あるいは拒絶されることになる。

【0042】

図6はこのアクセス制御を履行するため必要な高水準ステップである。ステップ401では、公開鍵証明書が検索された後、セキュリティ・サーバ101は特定の入力/出力アドレス指定を目標にしたプロキシ定義により、どのアトリビュート・フィルタが求められるか判定する。

【0043】

ステップ402では、セキュリティ・サーバ101はアトリビュート・フィルタが入力アドレスと関連があるか判定する。ステップ403で、セキュリティ・サーバ101が入力アドレスとの組み合わせを見つけたなら、このアトリビュート・フィルタは公開鍵証明書アトリビュートの評価を求めるアクセス演算式を持っているか判定するために再検討される。ステップ404では、アクセス演算式が評価される。ステップ406では、アクセス演算式が本物と評価したのでセキュリティ・サーバ101はどの保護リソース102へのアクセスも許可する。それ以外は、ステップ405で、アクセス演算式が偽物と評価したのでセキュリティ・サーバ101はアクセスを拒絶する。セキュリティ・サーバ101は接続要求を終了する。

【0044】

ステップ407では、アトリビュート・フィルタが出力アドレスとの関連があるとセキュリティ・サーバ101が判定したなら、同様のプロセスが続く。しかし、アクセスはその出力アドレスで特定の保護リソース102へだけ許可される。

【0045】

ステップ412では、アトリビュート・フィルタが入力アドレスか出力アドレスのどちらかと関連があるなら、アトリビュート・フィルタのプロセス処理は前述のように進行する。

【0046】

他の実施の形態への一般化

本発明は実行すべきステップ群やプロトコルに関して説明してきたが、本発明は上記説明のステップによりオペレーションをおこなうコンピュータ・システム、および上記説明のステップによりコンピュータ・システムがオペレーションをおこなうことが可能なソフトウェアを運搬するプログラム製品に属するものである。

【0047】

図では、ステップの順番は必ずしも厳密ではなく、あるステップは他のステップと並行、あるいは異なった順番でおこなうことが考えられる。

【0048】

特定の実施の形態を詳細に説明したが、本発明はそうした実施例に限定されるものではなく、添付の特許請求の範囲に基づき、公開鍵証明書アトリビュートが長所を引き立たせるように使用可能である。

【0049】

参照

1. 安全な電子商取引 (Secure Electronic Commerce)、W. フォード (Ford) と M. S. ボーム (Baum)、プレントス・ホール (Prentice Hall) PTR、1997。
2. インターネット RFC1960、「LDAP 検索フィルタのストリング表示 (A String Representation of LDAP Search Filters)」。

【図面の簡単な説明】

【図1】

保護リソースへのクライアント・ステーションからのアクセスを制限するためセキュリティ・サーバを使用する通常のコンピュータ・ネットワークを示す概略ブロック図。

【図2】

大人数ユーザ・システムに一般的に見られる特徴を組み込む、より洗練されたコンピュータ・システム・ネットワークを示す概略ブロック図。

【図3】

ユーザと、その特定のユーザで識別された公開鍵証明書との相関関係を説明する表。

【図4】

セキュリティ・サーバとクライアント・ステーション間の公開鍵と非公開鍵を用いた通常のユーザ・ログインおよび認証シーケンスを示す図。

【図5】

保護リソースへのアクセスを制御するため公開鍵証明書内のアトリビュートの使用を説明するフローチャート。

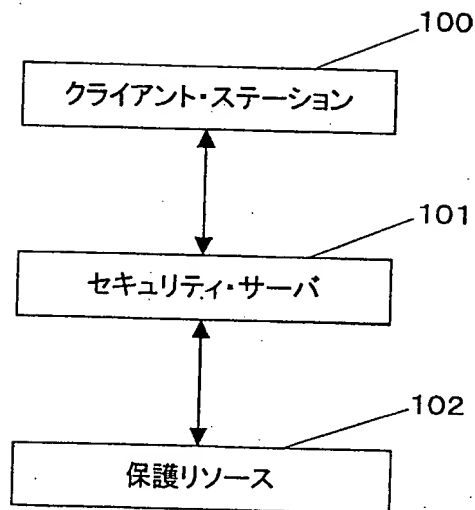
【図6】

保護リソースへのアクセスを制御するためプロキシ定義の入出力アトリビュートの使用を説明するフローチャート。

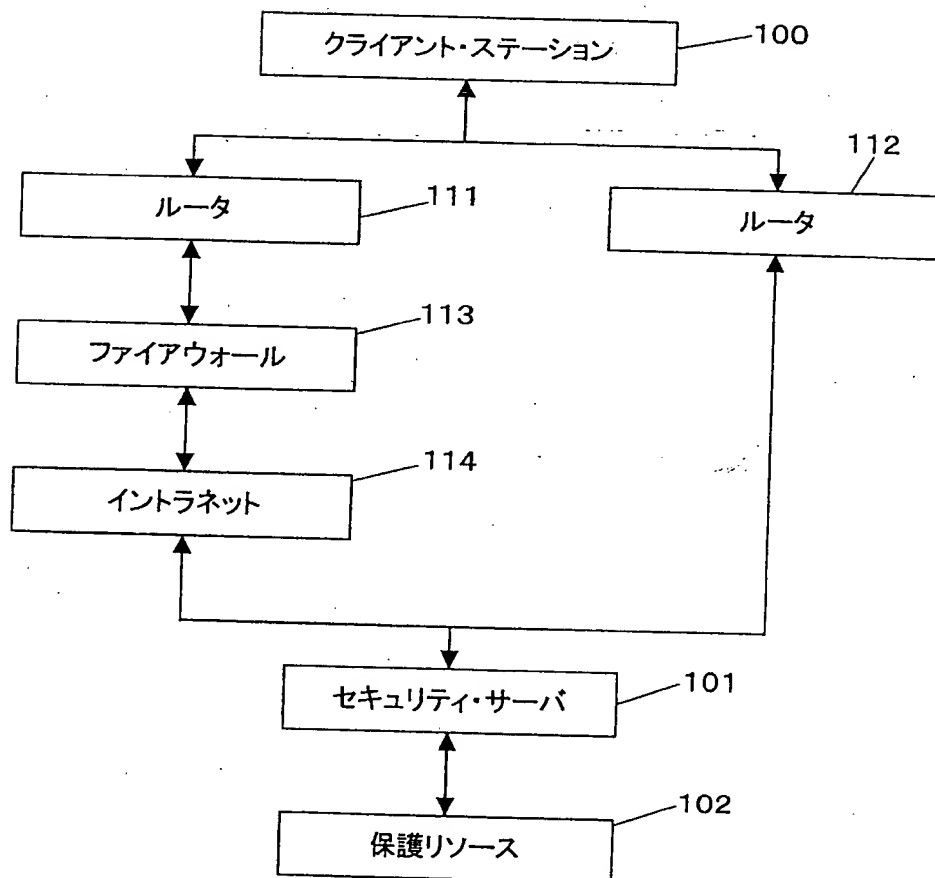
【符号の説明】

- 100 クライアント・ステーション
- 101 セキュリティ・サーバ
- 102 保護リソース
- 111 通信ルータ
- 112 通信ルータ
- 113 ファイアウォール
- 114 イン트라ネット

【図1】



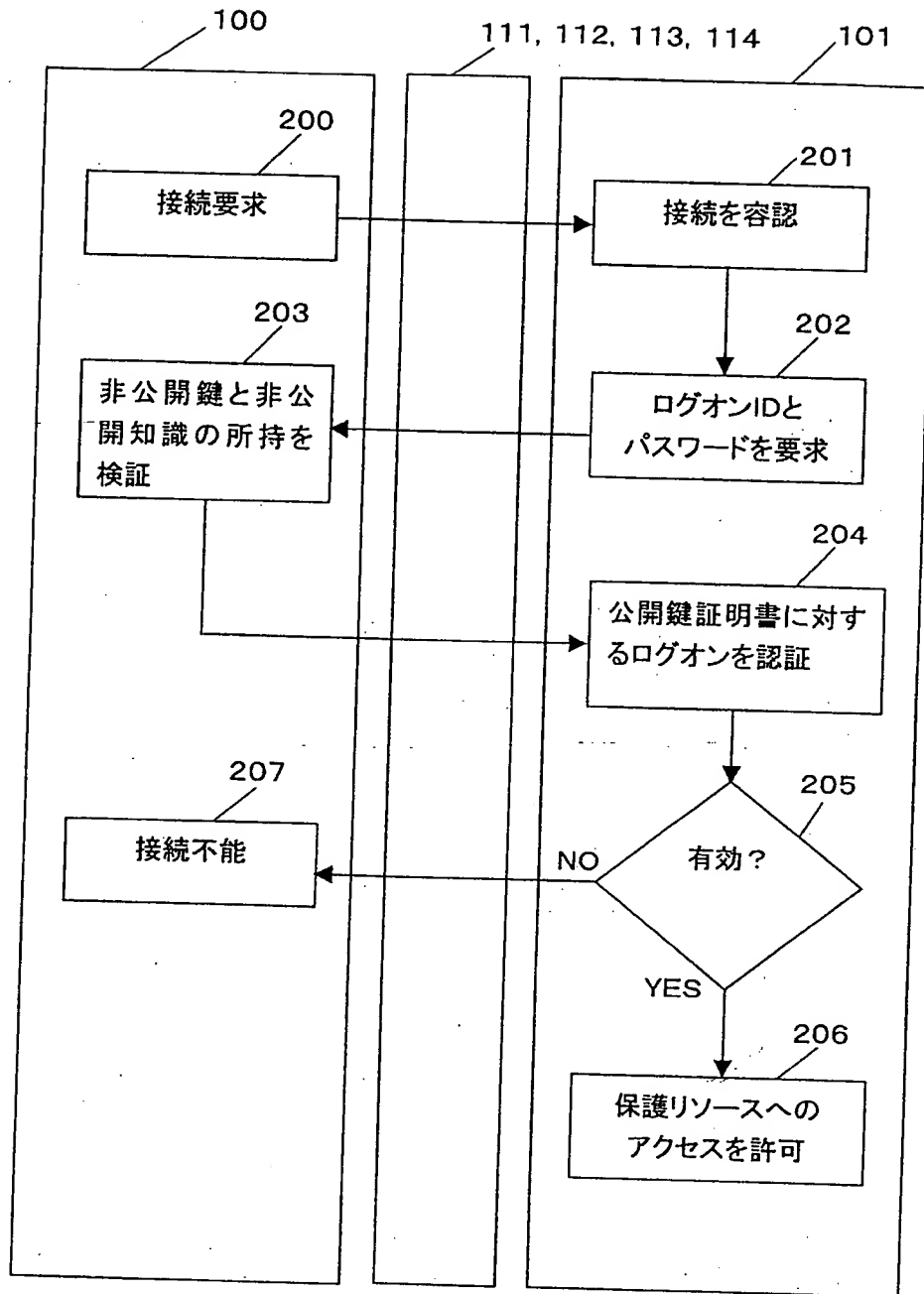
【図2】



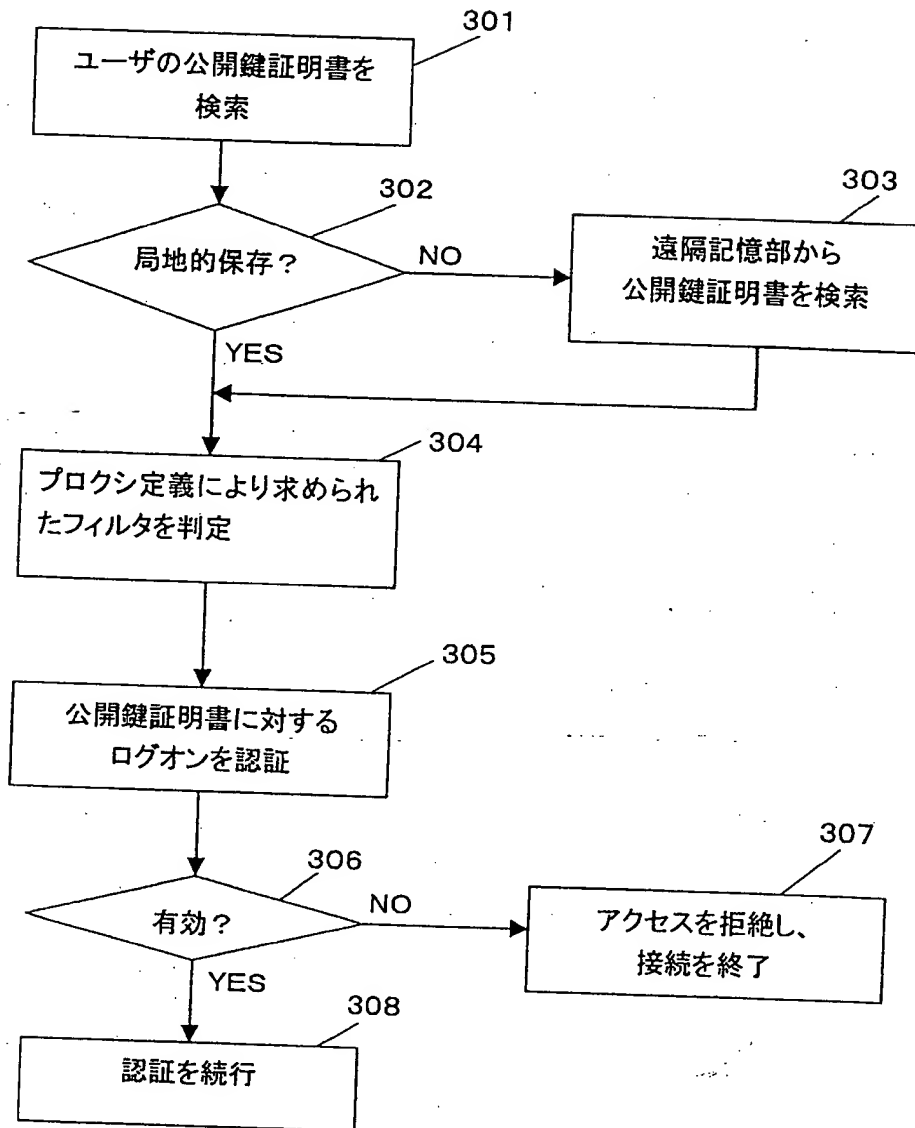
【図3】

証明書番号	ユーザ 名	公 開 鍵
1	ユーザ-1	公開鍵-1
2	ユーザ-2	公開鍵-2
3	ユーザ-3	公開鍵-3
4	ユーザ-4	公開鍵-4
n	ユーザ-n	公開鍵-n

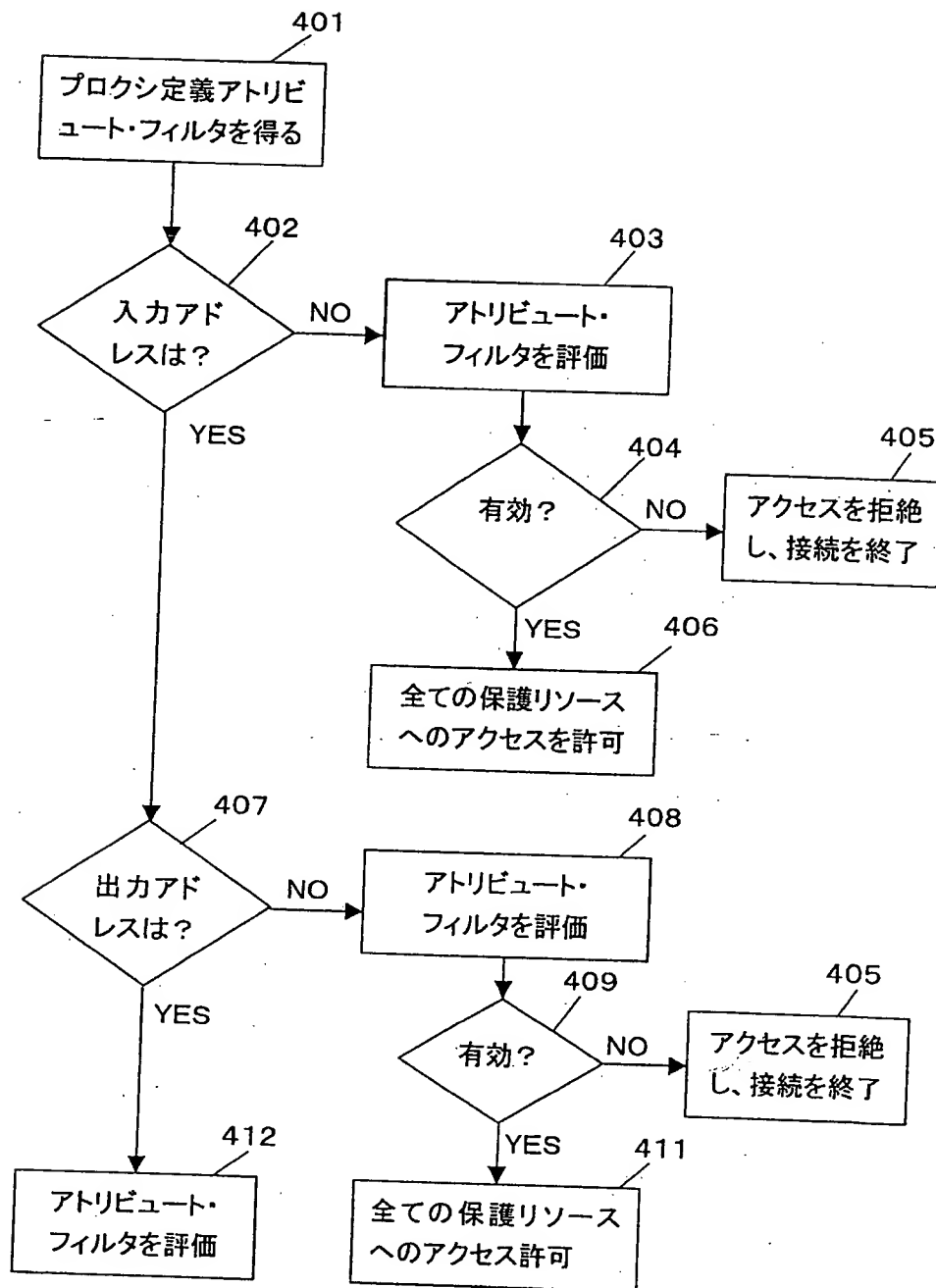
【図4】



【図5】



【図6】



【國際調查報告】

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 H04L29/06 H04L12/22		International Application No. PCT/IB 99/01452
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) IPC 7 H04L 606F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>PAYS P ET AL: "An intermediation and payment system technology"</p> <p>COMPUTER NETWORKS AND ISDN SYSTEMS, NL, NORTH HOLLAND PUBLISHING, AMSTERDAM,</p> <p>vol. 28, no. 11, page 1197-1206</p> <p>XP004018220</p> <p>ISSN: 0169-7552</p> <p>page 1199, right-hand column, line 19</p> <p>page 1201, left-hand column, line 24</p> <p>page 1202, right-hand column, line 15</p> <p>page 1204, left-hand column, line 13</p> <p style="text-align: center;">-/-</p>	1-33
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents:		
<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document relating to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principles or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family.</p>		
Date of the actual completion of the international search 17 December 1999		Date of mailing of the international search report 12/01/2000
Name and mailing address of the ISA European Patent Office, P.O. 5918 Patentlaan 2 NL - 2280 MV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016		Authorized officer Lázaro López, M.L.

Form PCT/ISA/210 (prevised sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		Inventor's Application No. PCT/IB 99/01452
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>WO 98 23062 A (NETIX INC T) 28 May 1998 (1998-05-28) page 7, line 28 - page 8, line 15 page 10, line 22 - page 12, line 19 page 13, line 20 - page 14, line 3 page 19, line 18 - page 20, line 9 page 21, line 17 - page 22, line 2 page 23, line 6-19 page 25, line 3 - page 29, line 4 page 31, line 8 - page 32, line 8</p>	1-33
A	<p>ANDERSON S ET AL: "Sessioneer: flexible session level authentication with off the shelf servers and clients" COMPUTER NETWORKS AND ISDN SYSTEMS, NL, NORTH HOLLAND PUBLISHING, AMSTERDAM, vol. 27, no. 6, page 1047-1053 XP004013206 ISSN: 0169-7552 page 1048, left-hand column, line 8 - page 1049, right-hand column, line 28 page 1050, left-hand column, line 32 - right-hand column, line 24</p>	1-33
A	<p>US 5 586 260 A (HU WEI-MING) 17 December 1996 (1996-12-17) column 1, line 47 - column 2, line 49 column 3, line 46 - column 5, line 3 column 5, line 65 - column 6, line 33</p>	1-33
A	<p>GARFINKEL S.: "Web Security & Commerce" June 1997 (1997-06), O'REILLY, USA XP002126084 page 151, line 5 - page 156, line 16</p>	1-33

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No.
PCT/IB 99/01452

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9823062 A	28-05-1998	AU 7304798 A EP 0938793 A	10-06-1998 01-09-1999
US 5586260 A	17-12-1996	NONE	